Open a Web Server to the Internet

Background

On May 1, 2023, all web servers open to the Internet must use Cloudflare or request an exception.

"Open Web Servers" are web servers that are visible from the Internet. Unless you take action to put the web server behind Cloudflare, it will only be visible from inside the Lab network. Web servers open to the Internet are challenging to secure due to ever increasing and sophisticated attacks. Even with careful configuration and updated software, new vulnerabilities emerge quickly. In order to protect web servers open to the Internet, they must be behind Cloudflare, which provides a wide range of protections.

Open Web Server Requirements

A summary of the requirements is below with more detail at Open Web Server Requirements.

1: Distinct server DNS record
2: Distinct website DNS record
3: Serving content
4: SSL configured

Request Cloudflare configuration

1. Complete the Cloudflare signup form. Cloudflare requests not meeting requirements will be rejected.
2. Cloudflare admins will create an appropriate record in Cloudflare. This record informs Cloudflare where it should send requests for the web site.
3. Cloudflare admins will use IP request to modify the web site DNS record you created to point to Cloudflare and change the TTL from 600 to 1800. For example, if your web site coolscience.lbl.gov is a CNAME to the target coolscience-local.lbl.gov, Cloudflare admins will change the target to coolscience.lbl.gov.cdn.cloudflare.net.
4. For web servers located in LBNL address space, Cloudflare admins will configure the Lab border rules to allow Cloudflare to access the IP for your server DNS record. Normally this command is run: acl-wired prefix $IP WAF-ALLOW-TCP443-IPv4
5. Cloudflare admins will reply to your request, normally the same day, but within 3 business days informing you the configuration is complete or that requirements are not met.

Exception Request

We recognize there are situations where Cloudflare is not an appropriate solution. Below are the identified categories of exceptions.

- Large Data Transfers - the primary purpose of the server is enabling file transfers, not serving html or user content. The most common cases are Globus (for transferring files) or perfSONAR (for bandwidth testing), but we recognize and allow exceptions for similar situations. In these cases, the costs (to pay Cloudflare) can increase significantly, outweighing the benefits of Cloudflare on an individual site.
- API endpoints - the primary purpose of the server is providing an API, not serving html or user content. We recognize many APIs do need additional protection, they are poorly designed and have serious vulnerabilities specific to them. Cloudflare has evolving set of tools to protect API's that we have not fully studied. API exceptions should be considered temporary exceptions that will be revisited as our understanding of Cloudflare API protections evolves.
- Equivalent controls - for whatever reason if you'd just prefer to avoid Cloudflare, the web server must be protected with compensating controls equivalent to those provided by Cloudflare. This includes (1) creating a mechanism to send your web server logs to Cyber, (2) implementing a Web Application Firewall (WAF), (3) implementing DDOS protection technology, (4) separating your server DNS record from your website DNS record, (5) meeting DHS BOD 18-01 requirements (HTTPS only, HSTS, Secure Ciphers), and (6) enabling your website to be protected in its entirety by the Lab SSO.

To request an exception, please email us the details of your exceptions, including the category of request above, for consideration at cloudflare@lbl.gov. Web servers that have been granted exceptions will have cloudflare-exceptions added as a DNS contact for tracking.

FAQ

1. How long after I make Cloudflare request until it becomes accessible from the Internet?

   Our goal is less than 3 business days.

2. Can I use a *DHCP host* as a web server?

   No. In order to have a web server be visible to the Internet, you must acquire a static IP address.

3. Who should I contact if I see a Cloudflare error?

   If you're a visitor to the site, as opposed to the admin, the best contact is the site's owner. LBL users can look up this information using https://dnscontacts.lbl.gov. If you're the site owner / administrator, you should contact cloudflare@lbl.gov.

4. What if I have questions?

   For questions or feedback please contact cloudflare@lbl.gov

5. What about Internet accessibility to other ports on my web server?

   Cloudflare will only proxy traffic for ports 80/tcp and 443/tcp to your web server hostname at this time. Internet accessibility to all other ports on the separate hostname (example-local.lbl.gov) is unaffected by this. For example, web visitors may access your web server at https://example.lbl.gov but you would SSH to it to manage it at example-local.lbl.gov. For more information, see #2 under Open Web Server Requirements. Keep in mind CPP always recommends you configure your computer for minimum exposure to the Internet, while meeting your business needs.
6. What if my hostname or IP change?

   If the hostname or IP address change, please email cloudflare@lbl.gov to have the Cloudflare records and LBNL border updated.

7. What about web servers on *non-standard ports*?

   We recognize that a web server can listen on any port, e.g. a non-standard port. Normally a web server listens on 80/tcp and a SSL enabled web server listens on port 443/tcp. The case where web servers run on non-standard ports is not addressed by Cloudflare at this time. If you would like to run a web server on a non-standard port, no Cloudflare is required.

8. I need to run some other application, that *is not a web server*, on 80/tcp or 443/tcp. Do I need to use Cloudflare?

   Yes. If you have some device or application that is not a web server and needs 80/tcp or 443/tcp to be visible from the Internet, it must be behind Cloudflare. For example, if you have a web camera that you control from the Internet via 443/tcp, the camera needs to be behind cloudflare

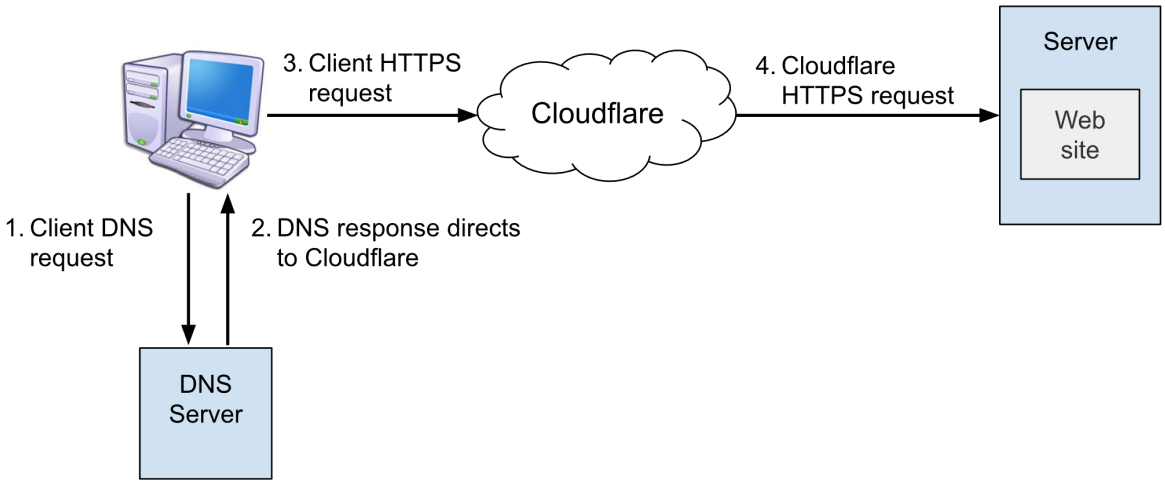
About Cloudflare

Cloudflare is a Reverse Proxy service that helps to protect Lab web servers, both hosted in the cloud and on-site. No additional fee is charged to utilize the Lab's Cloudflare service, but placing your web server behind it gets you many benefits:

- Web Application Firewall (WAF) filters out attacks from reaching your web server.
- Cyber Security logging grants us visibility into attacks against your web server.
- DDoS Protection keeps your server online in the event of a Distributed-Denial-of-Service attack.
- Caching continues to serve cached pages to end users even if your original server goes offline.
- Content Delivery Network speeds up your site by distributing resources to many Cloudflare servers around the world.

The high level Cloudflare process is shown below. As a results of the DNS request (1 and 2.) , the web request is sent to Cloudflare (3). Cloudflare cleans up the request and forwards it on to the Hostname running a Web Server (4).

Conceptual diagram



Terminology

Term	Definition
Client	Typically a Windows or Apple computer using a web browser such as Google Chrome
DNS Server	A server that has DNS records, commonly to resolve server names to IP addresses
Web site	The name put into a web browser to access your content, for example https://coolscience.lbl.gov
Server	A computer that offers network services, such as a web server or an SSH server. In the Cloudflare model, this must be separate from the web site name.

Open Web Servers	A server running a web site that is open to the Internet.
Internet	Any address space outside 128.3.0.0/16 and 131.243.0.0/16, which is the Berkeley Lab wired network.

Help/Feedback

If you have questions or comments about this website, please contact security@lbl.gov.

If you need general computer assistance, please contact the LBNL Help Desk at x4357, help@lbl.gov, or online at .